UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information Associated with Particular Cellular Towers

Case No. MJ20-427

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, incorporated herein by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 641	Theft of Public Property
18 U.S.C. § 1956	Money Laundering
18 U.S.C. § 1028A	Aggravated Identity Theft

The application is based on these facts:

✓ See Affidavit of SSA-OIG Special Agent Joseph Rogers, continued on the attached sheet.

☑ Delayed notice of 90 days (give exact ending date if more than 30 days: 10/13/2020 is requested under 18 U.S.C. § 3103a basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Joseph Rogers, SSA-OIG Special Agent
Printed name and title

○ The foregoing affidavit was sworn to before me and signed in my presence, or
◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 7/15/20

Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, Chief United States Magistrate Judge
Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Joseph Rogers, a Special Agent with the Social Security Administration, Office of the Inspector General in Seattle Washington, having been duly sworn, state as follows:

INTRODUCTION

1. I am a Special Agent with the Social Security Administration, Office of the Inspector General (SSA-OIG), stationed in Seattle, Washington and have been so employed since approximately June, 2003. I graduated from the Federal Law Enforcement Training Center (FLETC) in 2000, and since that time have had regular training in the enforcement of laws of the United States, including training in the preparation, presentation, and service of criminal complaints, arrests, and search warrants. I am a Certified Fraud Examiner. In addition to all aspects of Social Security fraud, I have extensive experience conducing criminal investigations relating to bank fraud, identity theft, theft of public funds, wire fraud, mail fraud, and other crimes.

2. I am investigating a massive fraud on the Washington Employment Security Department (ESD). The fraud involves the theft of hundreds of millions of dollars that were intended to provide economic relief to Washington workers affected by the COVID-19 pandemic. The investigation has revealed that criminals submitted thousands of fraudulent unemployment claims to ESD using the stolen personal identifying information of unwitting third persons. The fraudulent applications requested that the benefits be paid to bank accounts and payment cards controlled by persons known as "money mules," who withdrew and further dissipated the funds. The conduct under investigation violated numerous federal criminal statutes, including 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 641 (theft of public funds), 18 U.S.C. § 1956 (money laundering) and 18 U.S.C. § 1028A (aggravated identity theft).

3. I make this affidavit in support of an application for warrants for records and information associated with certain cellular towers ("cell towers"). The purpose of the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

warrants is to identify two persons (a money mule and a person believed to be supervising the money mule) who participated in the withdrawal of fraudulent ESD benefits. The cell tower data is expected to allow investigators to identify the phones used by the subjects at the time of the withdrawal, which may allow investigators to identify the subjects themselves.

4. The information requested is in the possession, custody, and/or control of T-Mobile, a cellular service provider headquartered in Bellevue, WA; Sprint, a cellular service provider headquartered in Overland Park, KS; Verizon Wireless, a cellular service provider headquartered in New York, NY; and AT&T Wireless, a cellular service provider headquartered in Dallas, TX. As described in the following paragraphs and in Attachment A, the requested warrant would require the disclosure of records and information relating to the cell towers providing service at the following locations as specified below:

Address	Date	Time Range
7451 Cirque Dr. W, University Place, WA 98467	May 3, 2020	4:25 PM PDT to 5:00 PM PDT
9518 176th St. E, Puyallup, WA 98375	May 6, 2020	2:40 PM PDT to 3:10 PM PDT
1112 South M St., Tacoma, WA 98405	May 11, 2020	1:20 PM PDT to 2:00 PM PDT
7250 Pacific Ave., Tacoma, WA 98408	May 11, 2020	2:35 PM PDT to 3:00 PM PDT

5. The information to be searched is described above and in Attachment A. This affidavit is made in support of an application for search warrants under 18 U.S.C. § 2703(c)(1)(A) to require T-Mobile, Sprint, Verizon Wireless, and AT&T Wireless to disclose to the government the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

6. The information set forth in this affidavit is not intended to detail each and every fact and circumstance of the investigation or all information known to me or the investigative participants. Rather, this affidavit is intended to present the facts relevant to the issue of whether probable cause exists to issue the requested search warrants.

7. This Court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

STATEMENT OF PROBABLE CAUSE

A. The CARES Act

8. Based on publicly-available information, I know that on March 27, 2020, the United States enacted into law the Coronavirus Aid, Relief, and Economic Security (CARES) Act. The CARES Act authorized approximately $2 trillion in aid to American workers, families, and businesses to mitigate the economic consequences of the COVID-19 pandemic. The CARES Act funded and authorized each state to administer new unemployment benefits. These benefits include (1) Federal Pandemic Unemployment Compensation (FPUC), which provides an additional benefit of $600 per week per unemployed worker; (2) Pandemic Unemployment Assistance (PUA), which extends benefits to self-employed persons, independent contractors, and others; and (3) Pandemic Emergency Unemployment Assistance (PEUC), which extends benefits for an additional 13 weeks after regular unemployment benefits are exhausted. All of these programs will be referenced herein as "CARES Act benefits." The CARES Act allows an unemployed worker to obtain back benefits retroactive to the date on which the applicant was affected by COVID 19, which, under program rules, may be as early as February 2, 2020.

9. The Washington Employment Security Department is the component of the State of Washington responsible for administering unemployment benefits, including CARES Act benefits. Applicants apply for ESD-administered benefits using ESD's Secure Access Washington (SAW) web portal. To submit an application, the applicant must enter his or her

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

personal identifying information (including name, date of birth, and Social Security number). ESD checks this information against its database of Washington residents. If ESD confirms that the information matches the personal identifying information of a person in ESD's records, ESD will pay out benefits via wire (ACH) transfer to an account identified by the applicant.

10. Prior to March 2020, before paying unemployment benefits to a worker, ESD generally required the worker's employer to provide confirmation that the employee had ceased working for the employer, and further, that the circumstances surrounding the termination rendered the employee eligible for unemployment assistance. However, in or about March 2020, as a result of changes in eligibility resulting from the CARES Act, and in an effort to distribute funds as quickly as possible, ESD stopped requiring employer verification before it paid claims.

B. Overview of Investigation

11. Beginning on around April 20, 2020, law enforcement officials began receiving complaints from employers about potentially fraudulent unemployment claims. The employers reported that they had received notices from ESD indicating that persons still under their employ had filed unemployment claims. For example, on or about April 20, 2020, the Seattle Fire Department (SFD) notified the U.S. Attorney's Office for the Western District of Washington that claims had been filed in the names of multiple firefighters who were actively employed by SFD. SFD reported that it had interviewed the firefighters, who had denied any involvement in the claims. Other employers, including Microsoft Corporation, the City of Bellingham, Zulily, and Seattle Yacht Club submitted similar complaints. The United States Attorney's Office referred the investigation to SSA-OIG on or about April 21, 2020.

12. Beginning on or about April 21, 2020, I notified ESD of the information provided by employers. I also requested that ESD provide me with claims data for the limited population of claims that were then known to be fraudulent. In reviewing the data, I noticed that a significant portion (approximately 35%) of the known fraudulent payments were made to Green Dot cards. Green Dot cards are prepaid payment cards that can be purchased at retail

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

locations such as Walgreens or Wal-Mart. After the buyer purchases the Green Dot card, he or she can fund the card through ACH (wire) transfers.

13. I contacted representatives of Green Dot and notified them that I had observed a pattern of fraudulent ESD payments being loaded onto Green Dot cards. Green Dot conducted research into its own data to identify other instances of fraud. Through a series of conversations with Green Dot fraud investigators over the next several weeks, Green Dot advised me that it had identified in excess of $150 million of ESD payments to Green Dot accounts that Green Dot had determined to be fraudulent. The vast majority of these payments were directed to Green Dot cards that had been purchased in states other than Washington, and particularly states in the Southeast region of the United States. In many cases, batches of cards were purchased at a single time, and then ESD benefits were loaded onto multiple cards in the same batch. Further, many of the cards had received payments issued on behalf of multiple beneficiaries.

14. Numerous other agencies, including the Federal Bureau of Investigation, the United States Secret Service, the Department of Labor Office of the Inspector General, the United States Postal Inspection Service, and Internal Revenue Service Criminal Investigation, joined the investigation. Agents from these agencies, including myself, have reviewed voluminous financial records and databases reflecting the fraudulent transactions and have conducted dozens of interviews.

15. One key source of data in the investigation is a database produced by ESD containing claims information of all claims currently believed to be fraudulent. ESD has updated this database several times. The most recent version (prepared on June 30, 2020) identifies 203,863 fraudulent claims. Based on interviews with ESD personnel, I understand that the claims listed in the database have been verified as fraudulent either because: (a) the purported claimant has verified for ESD that he or she did not submit the claim, or (b) the employer has verified for ESD that the claimant is not unemployed. I have used the database to generate numerous leads, and my investigative activities have confirmed that, for those leads I have investigated, the claims are indeed fraudulent.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

16. The database contains payment information indicating that the fraudulent benefit payments were made to thousands of banks around the country. Using that account information, agents have interviewed dozens of persons whose bank accounts received the fraud proceeds. Investigators refer to these persons as "money mules." In many or most cases, the money mules appear to be different from the persons who submitted the fraudulent claims. Many of the money mules are unwitting money mules, that is, they themselves are victims of romance or employment scams and are acting at the direction of others. For example, the money mule may believe that the benefit payment was deposited into his or her account by an online boyfriend or girlfriend, who requests that the money mule withdraw the money and send it to another account. The money mules typically withdraw the fraud proceeds shortly after the proceeds are deposited and then transfer the money according to instructions they receive.

17. The total amount of fraudulent claims paid out by ESD is currently unknown. However, the ESD's Commissioner, Suzi LeVine, has publicly stated ESD has paid out in excess of $500 million in fraudulent claims.

C. Identification of Green Dot Cards Used in the Fraud

18. As noted above, the perpetrators directed fraudulent benefit payments to accounts or financial institutions of their choosing, and the investigation has shown that many used online financial companies that issue pre-paid debit cards in order to facilitate expeditious and anonymous access to the fraudulent benefits paid. The largest of these companies, and the one most commonly used in connection with the fraud on ESD, is Green Dot. As noted above, Green Dot has provided investigators extensive records relating to thousands of accounts used to receive fraudulent ESD benefit funds, covering over one hundred million dollars in fraud.

19. Green Dot further reported that many of the cards that were activated and used for this fraudulent activity were purchased in groups of a dozen or more at a time from retail locations, such as Walgreens, CVS, and Walmart, throughout the United States. Green Dot representatives believed that the fact that the cards were purchased in batches was further evidence that the cards were purchased for the purpose of facilitating fraudulent activity, since

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

a legitimate unemployment claimant would not be involved in filing multiple claims. The investigation to date has shown that the person who purchases the group of Green Dot cards is typically a "handler" who may have multiple co-conspirators working for them by conducting transactions to withdraw the funds from the Green Dot cards, including through ATM withdrawals or the purchase of money orders.

20. On approximately June 23, 2020, I received information from Tacoma Police Department that a victim with the initials P.P., who resides in Western Washington, reported his personal information had been used to file a fraudulent unemployment claim, and that approximately $8,300 had been paid on the fraudulent claim. According to records provided by ESD and Green Dot, the benefits were paid to a Green Dot card ending in the numbers 0564 that was issued on May 3, 2020 using name and other identifying information of P.P. The fraudulent unemployment benefits deposited onto the card were as follows: $1,390 on May 5, 2020; $1,390 on May 11, 2020; and $5,530 on May 11, 2020. The information from Green Dot also showed that the funds were withdrawn from the Green Dot card through the following transactions: $1,390.96 on May 6, 2020 from WinCo Foods in Puyallup, WA; $2,952.64 on May 11, 202 from Fred-Meyer in Tacoma WA; and $2,504.45 on May 11, 2020 from Safeway in Tacoma, WA.

21. I also received information from Green Dot that the card ending in 0564 was purchased for cash on May 3, 2020, at a Walgreens Store in University Place, WA, and that the card ending in 0564 was one of a dozen Green Dot cards purchased during the same cash transaction.

D. Surveillance Footage of Green Dot Transactions

22. I obtained transaction data and security footage from the Walgreens located at 7451 Cirque Drive West, University Place, WA, related to the purchase of the dozen Green Dot cards, including the Green Dot card ending in 0564, on May 3, 2020. A review of the video showed a black male with a moustache and goatee (he was not wearing a COVID mask) purchasing approximately 12 Green Dot cards and paying for them with cash at approximately

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

4:50 PM PDT. While exiting the store, a good surveillance image of the subject can been seen. This subject will be referred to in this Affidavit as "Subject A."

23. WinCo Foods provided me surveillance photos from the security system of the store located at 9518 176th Street East, Puyallup, WA, showing the person who used the Green Dot card ending in 0564 to conduct the May 6, 2020, $1,390.96 transaction described above. The photos showed a black male walking inside the store, being assisted at the customer service desk, and exiting the store. While in the store, the subject used the Green Dot card ending in 0564 to purchase two Western Union money orders at approximately 2:55 PM PDT: one in the amount of $390 with a payee of "Michael Davy" handwritten in; and one in the amount of $1,000 with a payee of "W&L Affordable Auto" handwritten in. The black male was wearing a tan hat with a Seahawks logo on the front, and a COVID mask. However, while exiting the store, he removed the mask and his face can be seen. This was a different individual than Subject A (who originally purchased the Green Dot cards at the University Place Walgreens), and will be referred to hereafter as "Subject B." The surveillance photos from outside the store showed Subject B get into the passenger seat of an unidentifiable vehicle.

24. I also received security surveillance photos from the Safeway store located at 1112 South M Street, Tacoma, WA showing the person who used the Green Dot card ending in 0564 to conduct the May 11, 2020 $2,504.45 transaction described above. The photos showed a black male walking inside the store, being assisted at the customer service desk, and exiting the store. The male was wearing a COVID mask, dark blue shorts, a t-shirt that with the words "Just Do It" and the Nike Logo across it, and a dark blue hat with a dark blue Seahawks Logo on the front. The Seahawks hat was a different color than the one worn by the subject who purchased the money orders at WinCo Foods on May 6, 2020; however, even though this subject did not remove his COVID mask, the Safeway subject's build and appearance was the same as the person purchasing the money orders at WinCo Foods; that is to say, Subject B. Subject B used the Green Dot Card ending in 0564 and purchased five Western Union money orders: four in the amounts of $500 with a payee of "H&S" handwritten

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

in; and one in the amount of $500 with a payee of "W&L Affordable Auto" handwritten in (the same amount and payee as one of the money orders purchased on May 6, at WinCo, described above).

25. I obtained and reviewed the security video from the Tacoma Safeway during Subject B's May 11 visit. The video showed that Subject B was at that location with, and in contact with, Subject A, the person who initially purchased the set of Green Dot cards from the University Place Walgreens on May 3, 2020. Specifically, the video showed the following:

a. At approximately 1:28 PM PDT, the video of the outside parking lot of the Safeway shows a newer grey Dodge Challenger moving in the parking lot and parking in a spot. The driver's door opened and several persons from the parking lot approached the vehicle and talked to the driver.

b. While this was happening, an individual, later identified as Subject B, as described below, arrived at the Safeway at approximately 1:29 PM PDT, driving an older silver SUV. Subject B drove to the farthest parking row from the store, parked, and remained inside his vehicle.

c. At approximately 1:30 PM PDT, the driver of the Dodge Challenger, later identified as Subject A, as described below, walked into Safeway. (While Subject A was walking into the store, he can be seen looking at his cellular phone.) At approximately 1:32 PM PDT, Subject A exited the store, walked around to the passenger side of his vehicle and looked towards where Subject B was parked. Subject A can be seen carrying a cell phone in his right hand while walking from the store to his car. Subject A was not wearing a COVID mask and clear images of his face can be seen on the video. He is a black male with a moustache and goatee, and matched the appearance of the individual observed purchasing the dozen Green Dot cards at the University Place Walgreens on May 3, 2020.

d. As Subject A entered the driver's side of his vehicle, Subject B left his vehicle and walked towards Safeway, walking behind Subject A's vehicle without making contact with Subject A or otherwise acknowledging him. Once inside Safeway, Subject B went right to the customer service desk. While Subject B was waiting in line he can be seen

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

texting on his phone. Subject B purchased the money orders, as described above, and left the store at approximately 1:44 PM, PDT. The surveillance images clearly showed Subject B carrying the papers, assumed to be the purchased Western Union money orders, in his right hand. He can again be seen texting with his phone in his left hand while exiting the store.

e. After leaving the store, Subject B walked directly to Subject A's vehicle (the Dodge Challenger) and leaned into the vehicle through the open driver's window. After this contact, Subject B no longer had any papers visible in either of his hands, so it is presumed the money orders were given to Subject A. Subject B then walked to his vehicle and entered the driver's side. At approximately 1:45 PM, PDT, Subject A drove away. At approximately 1:52 PM PDT, Subject B drove away.

26. Based on my training and experience, and the observations described above, I believe that Subject A acted as a "handler" of Subject B, purchasing the Green Dot cards that were subsequently loaded with fraudulent unemployment benefits money, then at some point providing at least the card ending 0564 to Subject B, who used it to purchase money orders from Safeway while Subject A waited outside. Subject A then received the purchased money orders from Subject B after the transaction was completed.

27. Fred Meyer provided me surveillance photos from the security system of their store located at 7520 Pacific Avenue, Tacoma, WA, showing the person who made the May 11, 2020 $2,952.64 purchase with Green Dot card ending in 0564. This transaction took place roughly one hour after the transaction at Safeway, described above, at approximately 2:45 PM PDT. The surveillance photos showed a black male walking inside the store and being assisted at the customer service desk. The black male was wearing a COVID mask, but was wearing the same clothing, including the same dark Seahawks hat, Just Do It t-shirt, and dark shorts, as the individual observed earlier in the afternoon at the Tacoma Safeway; that is to say, Subject B. Subject B used the Green Dot card ending in 0564 to purchase three Western Union money orders: one in the amount of $1,000 with a payee of "H&S" handwritten in (the same payee as four of the money orders purchased earlier the same afternoon at Safeway, as

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

described above); one in the amount of $1,000 with a payee of "Elite Casting Inc." handwritten in; and one in the amount of $950 with the payee "IAA" handwritten in.

28. While the investigation has visually identified Subjects A and B as participants in the fraud scheme, their identities are unknown at this time. However, for each Subject, investigators know at least two specific times and locations the Subject was present. These are the times and locations described further in Attachment A (specifically, at the University Place Walgreens (May 3, 2020) and the Tacoma Safeway (May 11, 2020) for Subject A; and at the Puyallup WinCo (May 6, 2020), Tacoma Safeway (May 11, 2020), and Tacoma Fred Meyer (May 11, 2020) for Subject B). Cellular tower data from the locations of these four stores, at the approximate times of the observed transactions, will permit investigators to identify common cellular phones located across these transactions. That is, if the same cell phone was used at two of these locations at times the Subject was known to be present at each respective location, it is reasonable to conclude that that cell phone was being used by the subject. Moreover, based on my training and experience, the meeting of Subjects A and B, driving two separate cars, at the Tacoma Safeway (where both subjects were observed carrying cellular phones, and where Subject B was observed using his phone), likely involved the use of cellular phones by the Subjects to communicate and coordinate with one another. The requested data will therefore assist investigators both in identifying the subjects and in identifying any communications with one another.

E. Background on Cell Towers

23. In my training and experience, I have learned that T-Mobile, Sprint, Verizon Wireless, and AT&T Wireless are companies that provide cellular communications service to the general public. In order to provide this service, many cellular service providers maintain antenna towers ("cell towers") that serve and provide cellular service to devices that are within range of the tower's signals. Each cell tower receives signals from wireless devices, such as cellular phones, in its general vicinity. By communicating with a cell tower, a wireless device can transmit and receive communications, such as phone calls, text messages, and other data.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

When sending or receiving communications, a cellular device does not always utilize the cell tower that is closest to it.

24. Based on my training and experience, I also know that each cellular device is identified by one or more unique identifiers. For example, with respect to a cellular phone, the phone will be assigned both a unique telephone number but also one or more other identifiers such as an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), a Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Equipment Identity ("IMEI"). The types of identifiers assigned to a given cellular device are dependent on the device and the cellular network on which it operates.

25. Based on my training and experience, I know that cellular providers, such as T-Mobile, Sprint, Verizon Wireless, and AT&T Wireless, routinely and in their regular course of business maintain historical records that allow them to determine which wireless devices used cellular towers on the cellular provider's network to send or receive communications. For each communication sent or received via the wireless provider's network, these records may include: (1) the telephone call number and unique identifiers of the wireless device that connected to the provider's cellular tower and sent or received the communication ("the locally served wireless device"); (2) the cellular tower(s) on the provider's network, as well as the "sector" (*i.e.*, face of the tower), to which the locally served wireless device connected when sending or receiving the communication; and (3) the date, time, and duration of the communication.

26. Based on my training and experience, I know that cellular providers, such as T-Mobile, Sprint, Verizon Wireless, and AT&T Wireless, have the ability to query their historical records to determine which cellular device(s) connected to a particular cellular tower during a given period of time and to produce the information described above. I also know that cellular providers have the ability to determine which cellular tower(s) provided coverage to a given location at a particular time,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

27. Based on my training and experience and the above facts, information obtained from cellular service providers such as T-Mobile, Sprint, Verizon Wireless, and AT&T Wireless that reveals which devices used a particular cell tower (and, where applicable, sector) to engage in particular communications can be used to show that such devices were in the general vicinity of the cell tower at the time the communication occurred. Thus, the records described in Attachment A will identify the cellular devices that were in the vicinity of the four stores at which the Green Dot card ending 0564, used for accessing fraudulent ESD benefits, was purchased and/or used at the specific times that those transactions in furtherance of the fraud were taking place. This information, in turn, will assist law enforcement in determining which persons were present for those transactions.

28. The data provided by the cell providers will, of necessity, include cell phone data of persons not associated with the fraud, who happened to be in the same locations as the Subjects at the timers described above. However, the requested warrant protects the privacy of those persons by only authorizing the seizure of cell phone data for accounts relevant to phones that (a) used more than one tower identified by the government during the specified time periods; or (b) communicated with a phone that used more than one tower identified by the government during the specified time periods.

AUTHORIZATION REQUEST

29. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c).

30. I further request that the Court direct T-Mobile, Sprint, Verizon Wireless, and AT&T Wireless to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on T-Mobile, Sprint, Verizon Wireless, and AT&T Wireless, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

REQUEST FOR NONDISCLOSURE AND SEALING

29. The government requests, pursuant to the preclusion of notice provisions of Title 18, United States Code, Section 2705(b), that the cellular service providers be ordered not to notify any person (including the subscriber or customer to which the information may relate) of the existence of this warrant for such period as the Court deems appropriate. In this case, such an order is appropriate because the search warrants relate to an ongoing criminal investigation and disclosure would provide the targets with information about the government's investigation that could be used to frustrate further investigative efforts.

30. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. There is good cause to seal these documents because their premature disclosure may give the subjects an opportunity to flee from prosecution, dissipate assets, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

31. For these reasons, I am requesting that the Court issue an order sealing the search warrant, search warrant return, application and affidavit for the search warrant, and all attachments.

CONCLUSION

32. Based on the forgoing, I request that the Court issue the proposed search warrants. This Court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of these warrants. The government will execute these warrants by serving the warrants on the cellular service providers listed in Attachment A. Because the warrants will be served on those cellular service providers, which will then compile the requested records at

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

a time convenient to them, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

33. Accordingly, by this Affidavit and requested warrants, I seek authority for the government to search all of the items specified in Section I, Attachment B (attached hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents and records that are identified in Section II to that same Attachment.

JOSEPH ROGERS, Affiant
Special Agent
Social Security Administration
Office of Inspector General

The above-named agent provided a sworn statement to the truth of the foregoing affidavit by telephone on 15th day of July 2020.

HONORABLE BRIAN A TSUCHIDA
Chief United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Property to Be Searched

Records and information associated with communications to and from the following cellular antenna towers ("cell towers") on the identified dates and timeframes that are within the possession, custody, or control of the cellular service providers identified below:

Cell Towers	Dates	Times (PDT)
The cell towers that provided cellular service to 7451 Cirque Dr. W, University Place, WA, 98467	May 3, 2020	4:25 PM to 5:00 PM
The cell towers that provided cellular service to 9518 176th St. E, Puyallup, WA, 98375	May 6, 2020	2:40 PM to 3:10 PM
The cell towers that provided cellular service to 1112 South M St., Tacoma, WA, 98405	May 11, 2020	1:20 PM to 2:00 PM
The cell towers that provided cellular service to 7250 Pacific Ave., Tacoma, WA, 98408	May 11, 2020	2:35 PM to 3:00 PM

The following cellular service providers are required to disclose information to the United States pursuant to this warrant:

1. T-Mobile, a cellular service provider headquartered in Bellevue, WA;
2. Sprint, a cellular service provider headquartered in Overland Park, KS;
3. Verizon Wireless, a cellular service provider headquartered in New York, NY; and
4. AT&T Wireless, a cellular service provider headquartered in Dallas, TX.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

For each cell tower described in Attachment A, the cellular service providers identified in Attachment A are required to disclose to the United States records and other information (not including the contents of communications) about all communications made using the cellular towers) identified in Attachment A during the corresponding timeframes listed in Attachment A, including records that identify:

a. the telephone call number and unique identifiers for each wireless device in the vicinity of the cell tower ("the locally served wireless device") that registered with the cell tower, including Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), and International Mobile Equipment Identities ("IMEI");

b. for each communication, the "sectors" (i.e. the faces of the towers) that received a radio signal from the locally served wireless device;

c. the date, time, and duration of each communication.

These records should include records about communications that were initiated before or terminated after the timeframe(s) identified in Attachment A if some part of the communication occurred during the relevant timeframe(s) listed in Attachment A.

II. Information to be Seized by the Government

The government is authorized to review the data identified above to identify any cell phone accounts that were used in more than one of the times and places specified above (a "multiple hit account"). If the government identifies multiple hit account, it may further

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

search the data to identify any cell phone account that communicated with the multiple hit account during the specified times. The government is authorized to seize all information produced pursuant to this warrant that is associated with any multiple hit account and with any account communicating will a multiple hit account during the at the specified times and places.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970